# SECURE THE SECRET IMAGE IN VISUAL CRYPTOGRAPHY USING N- SHARES OF HALF TONE IMAGES

*S.Narmadha*, S.Sheeja*

## ABSTRACT

Visual cryptography is a technique that allows visual information to be encrypted and it can perform the decryption without any cryptographic information. Visual cryptography depends on the contrast, security, accuracy and complexity of the images. Data can be protected while transferring the data in wireless network. The images can be shuffled according to the position of the pixel values, and also it makes the complex relationship between the original images encrypted images. The XOR operation is performed to construct the secret image.

Keyword: Pixel Expansion, Visual cryptography, Watermarking

## I. INTRODUCTION

The visual cryptography is a way to encrypt the visual data without require any complex data calculations on the destination for maintaining the data in a confidential. Based on the principles of Naor and Shamir [1] to encrypt the digital images.

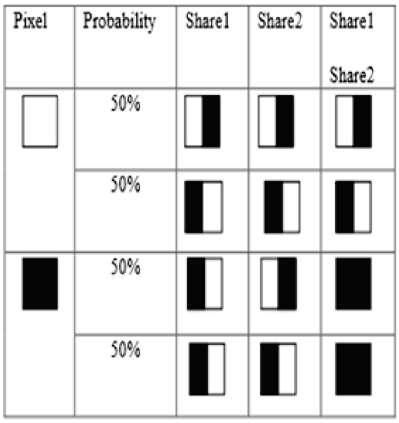


**Fig 1: Encrypt digital images**

## II. CRYPTOGRAPHY PRIMITIVIES

Cryptography is a technique that can be used to give a safety measure such as

1. Encryption
2. Hash function
3. Digital Signatures

The cryptosystem provides privacy to the information that being transferred. It depicts the following picture as follows,

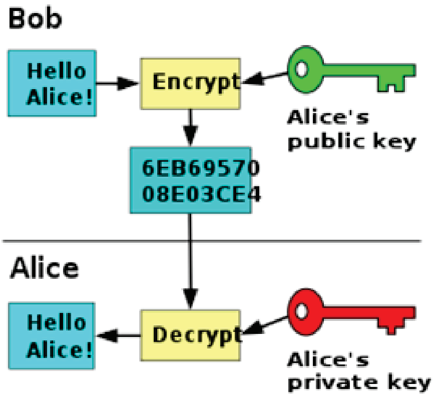


**Fig 2: Simple model of Cryptosystem**

The above diagram proceeds that sender can send the message to the receiver the third person can access the information but it could not find out. The sender can send the message with encryption using public key, While the receiver receives the same message can be decrypt using the private key. The receiver receives the original message that what sender has send to Destination.

## III. LITERATURE SURVEY

### Multiple Secret Sharing Scheme

This technique is used to distributing two secret photos over two shares in visual cryptography. Wu and Chen 1998[2] to present the visual cryptography schemes to share two secret images in two shares. The two shares of images can be stacked from one another. By rotating the one shares in 90 degree, the secret images can be obtained, same way the

Department of Computer Science
Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
*Corresponding Author

same image can be rotate in 180 or 270 degree, the secret images can be obtained. The images can give the high contrast and it gives high complexity with reduces the effectiveness for the real time applications.

To hide more than one piece of information in multiple secret schemes refereed as Dynamic visual cryptography.

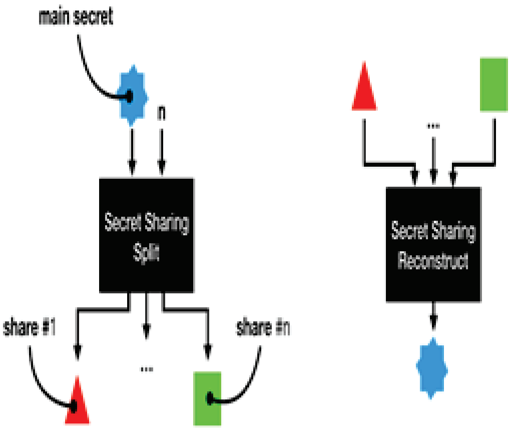


Fig 3: Multiple Secret Sharing Scheme

### Flip Based Cryptography

This technique is used for overlapping of the images of the two shares, the first secret images will produce. It encodes two secret images into share images. FVC was pioneered by Lin et al. in [3] In FVC, a pair of shares contains pixel information from two secret images.

### Performance Analysis of Visual Cryptography

It provides the two main parameters pixel expansion m and contrast. It represents the loss in resolution from the original images and it gives the good clarity of the images. Security is satisfied while there is no information can be reveals in each share of the original images. Computational complexity required the set of n shares and it can reconstruct the original images.

Yan, X., Wang [4] advised security, pixel expansion, accuracy and computational complexity as a performance measure. Security is satisfied if each share reveals no information of the original image and it cannot be reconstructed if there are fewer than k shares collected.The recovered images contain error free and lossless excellent image quality based on the Caser Cipher algorithm approach. The created shares of the original photos can be encrypted using RSA Algorithm.

To improve the security of VC, some schemes have merged between the VC and the Cryptography Techniques. Yadar and Ojha, [5] have proposed a scheme based on Caser Cipher algorithm and the concept of RG for gray level images. Shetty and Abraham [6] proposed a VC scheme which could be applied to both binary and color images. It was implemented on the basis of the traditional VC concept to generate two shares from the secret image after being converted to a binary- valued image. Then, RSA algorithm was performed to encrypt the generated shares, Here, the generated shares and recovered image had the same size of the original image.

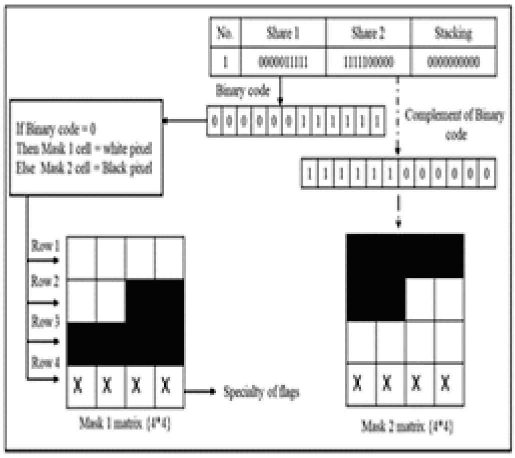
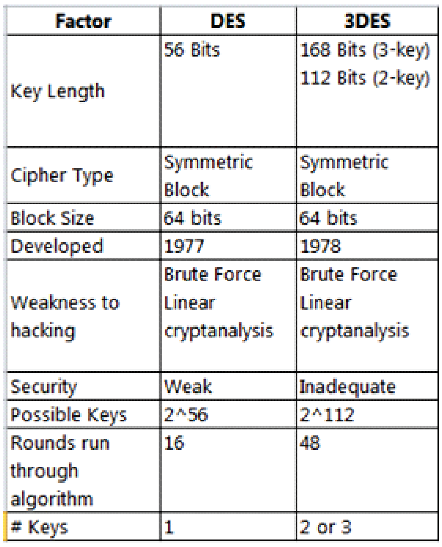


Fig 4: Create Mask 1[4,4] and mask 2[4,4] matrix in Hash codebook

## IV. PROPOSED METHODOLOGY

To generate a random share image, divide it into a mask cell with size= [4*4], in which the first three rows in the mask distribute the 12 bits of the binary image and proposed an Elliptic Curve Cryptography (ECC) based VSS scheme[7] in order to be applied on RGB images. Data encryption standard (DES) has been found vulnerable to very powerful attacks and therefore, the popularity of DES has been found slightly on the decline. DES is a block cipher and encrypts data in blocks of size of 64 bits each, which means 64 bits of plain text go as the input to DES, which produces 64 bits of ciphertext.



| Factor | DES | 3DES |
|---|---|---|
| Key Length | 56 Bits | 168 Bits (3-key)<br>112 Bits (2-key) |
| Cipher Type | Symmetric Block | Symmetric Block |
| Block Size | 64 bits | 64 bits |
| Developed | 1977 | 1978 |
| Weakness to hacking | Brute Force<br>Linear cryptanalysis | Brute Force<br>Linear cryptanalysis |
| Security | Weak | Inadequate |
| Possible Keys | 2^56 | 2^112 |
| Rounds run through algorithm | 16 | 48 |
| # Keys | 1 | 2 or 3 |

**Fig 5: Comparison of DES And TRIPLE DES**

The classic Hill Cipher has many merits. Some of these merits Some of the merits include the following: (1) it is resistant to the frequency latter analysis, (2) it provides high speed and high throughput. In spite of these merits, the non-invertible key matrix is the main demerit of the Hill Cipher because the encrypted text cannot be decrypted [8]. Another demerit is the linear nature which can make it to known – plaintext- attack.

It provides the high throughput of the images. The encrypted text cannot be decrypted. It gives a number of shares with the original images and provides gray scale images and RGB images [9]. Non – Invertible key matrix is used to strengthen the security level of the secret images. The degree of confidentiality determines the secrecy of the information. Availability of the information of shared images can be secured.

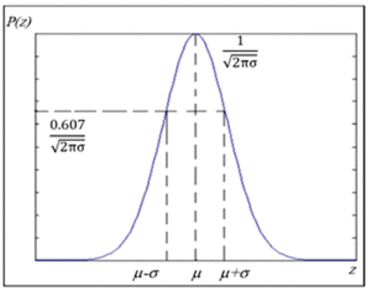


**Fig:6 An Optimization of color Halftone Visual Cryptography**

The lightweight block cipher represents a complete data block that is processed at once. The main concerns for evaluating a lightweight block cipher are block size, key size, number of rounds, and the type of structure. While lightweight stream cipher works on encrypting and decrypting data bit by bit and it is quicker and simpler than lightweight block cipher [10].

## V. FUTURE ANALYSIS

The shares can be produced by all the methods that can be produced by using method of multiple images in secret images. The proposed scheme can be improved by using segmentation of the images, and to increase the robustness. To improve the quality of the images by using the DES and Triple DES Algorithm.

## VI. CONCLUSION

The proposed system significantly performs and it produce the quality, contrast and reliability of the images. It will be used for the image copyright protection, secret communication in military, document authentication of the images, secret data storing.

## REFERENCES

1. Naor, M., Shamir, A.: Visual cryptography. In: Advances in Cryptology - EUROCRYPT'94, pp. 1–12. Springer Berlin Heidelberg (1995). DOI 10.1007/bfb0053419.

2. Wu C.C., L.H. Chen, "A Study On Visual Cryptography", Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C., 1998

3. Lin, S.J., Chen, S.K., Lin, J.C.: Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast, and no expansion. Journal of Visual Communication and Image Representation 21(8), 900–916 (2010). DOI 10.1016/j.jvcir.2010.08.006

4. Yan, X., Wang, S., Niu, X., Yang, C.N.: Generalized random grids-based threshold visual cryptography with meaningful shares. Signal Processing 109, 317–333 (2015). DOI 10.1016/j.sigpro.2014.12.002

5. Yadav, G.S., Ojha, A., 2013, December. A novel visual

cryptography scheme based on substitution cipher. In: Image Information Processing (ICIIP), 2013 IEEE Second International Conference on (pp. 640-643). IEEE.

6. Shetty, S., Abraham, M.P., April 2015. A Secure Visual Cryptography Scheme for Sharing Secret Image using RSA. Int. J. Innovative Res. Comput. Commun. Eng. 3 (4), 3331–3336.

7. Shankar, K., Eswaran, P., February 2017. RGB based multiple share creation in visual cryptography with aid of elliptic curve cryptography. China Commun. 14 (2), 118–130. https://doi.org/10.1109/CC.2017.7868160

8. Saturwar J, Chaudhari DN. Secure visual secret sharing scheme for color images using visual cryptography and digital watermarking. Second International Conference on Electrical, Computer and Communication Technologies (ICECCT). Vol. 4, Issue 3. India: IEEE; 2017. p.1–4.

9. Fadel H, Hameed RS, Hasoon JN, Mostafa SA, Khalaf BA. A light-weight ESalsa20 Ciphering based on 1D logistic and chebyshev chaotic maps. Solid State Technol. 2020;63(1):1078–93.

10. Ismael HA, Abbas JM, Mostafa SA, Fadel AH. An enhanced fireworks algorithm to generate prime key for multiple users in fingerprinting domain. Bull Electr Eng Inform. 2021;10(1):337–43.